SECURITY EDUCATION

INTRODUCTION TO ISO/SAE 21434

HPC/HCTD/HCTS/HCTSP
RENESAS ELECTRONICS CORPORATION

VERSION 2.0 (EN)
AST-BC-25-0003
MAY 15, 2025

 RENESAS CONFIDENTIAL

RENESAS

This training is an introduction to ISO/SAE 21434.

TABLE OF CONTENTS

1. Introduction p03
2. Planning p07
3. Development p11
4. Continual security activities p18
5. Foundation of security processes p20
6. Summary p25

Appendix p26

We will start by explaining the objectives,
then explain the requirements for each of the planning, development,
continual activities and process foundations, and finally summarise.

INTRODUCTION

Firstly, we‘ll explain its objective, scope and life cycle.

OBJECTIVE

This security education “Introduction to ISO/SAE 21434” provides:

1. overview of security requirements stated by ISO/SAE 21434
2. overview of work products required by ISO/SAE 21434

This security education does NOT provide the following:

1. foundamental security knowledge
2. Renesas development processes (RCT, TOS)
3. security features implemented in Renesas products (MCU, SoC)

Where above information is required, please refer to the corresponding security educations.

This tutorial provides an overview of the security requirements and work products required by ISO/SAE 21434.
It does not cover the fundamental knowledge development process or security functions.

APPLICATION SCOPE

The application of ISO/SAE 21434 is limited to electrical and electronic (E/E) systems in road vehicles and their interfaces.

External systems are out of scope.

Requirements are defined for the item corresponding to in-vehicle system and the components such as ECUs embedded in item.

There is no distinction between HW and SW in the requirements.

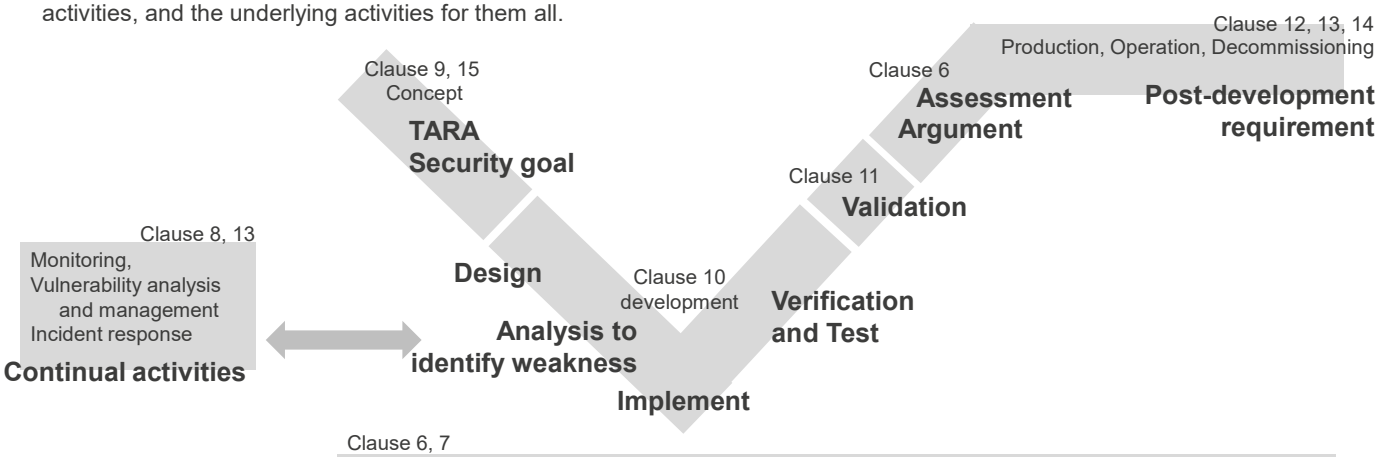
Tailoring of the standard requirements is required to apply them to the semiconductor and SW development processes.

The scope of ISO/SAE 21434 is limited to automotive electrical and electronic systems and their interfaces.
External systems such as servers are not covered.
Furthermore, each requirement of ISO/SAE 21434 is defined for items that correspond to in vehicle systems and components such as ECUs that are embedded in items.
ISO/SAE 21434 does not distinguish between hardware and software.
Each requirement must be tailored to fit the semiconductor and software development process.

TARA Threat Analysis and Risk Assessment
QM Quality Management

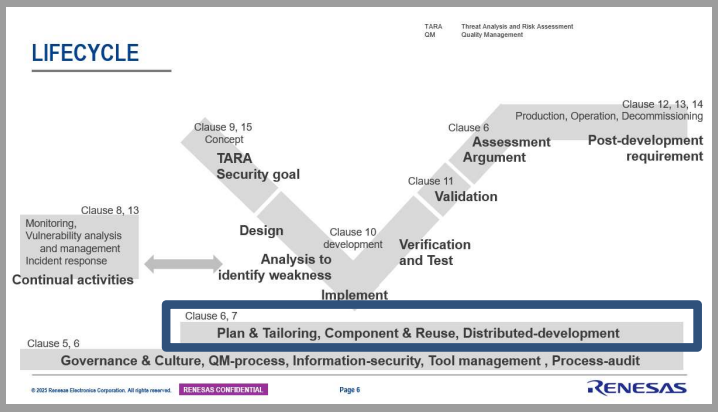
LIFECYCLE

ISO/SAE 21434 defines requirements for the complete product lifecycle, including product dev plan, V-model, continuous activities, and the underlying activities for them all.



ISO/SAE 21434 defines requirements for the complete life cycle, including the product development plan, the V model of development, the continual activities, and the foundation of all these processes.

PLANNING



This chapter explains cybersecurity planning and tailoring, components and their reuse, and the requirements for distributed development.

WP ID	Name
WP-06-01	Cybersecurity plan

PLAN AND TAILORING

Before development begins, each cybersecurity activity shall be examined, and a cybersecurity plan shall be created.

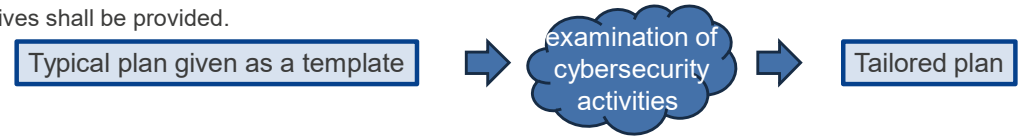
Cybersecurity plan shall include: RQ-06-03

- objective of each cybersecurity activity
- dependencies on other activities or information
- personnel responsible for performing each activity
- required resources for performing each activity
- starting point or end point, and the expected duration of each activity
- identification of the work products to be produced

RQ-06-02, RQ-06-10, RQ-06-14, etc.

Cybersecurity plan should be tailored by examining the cybersecurity activities, such as reuse & distributed development.

If a cybersecurity plan is tailored, then a rationale why the tailoring is appropriate and sufficient to achieve the relevant objectives shall be provided.



Cybersecurity plan should be updated incrementally as changes or refinements occur. RQ-06-07

A cybersecurity plan is created by examining each cybersecurity activity and tailoring it as necessary.
When tailoring is done, it is necessary to show the rationale why it is appropriate and sufficient.

COTS Commercial Off-The-Shelf (component)

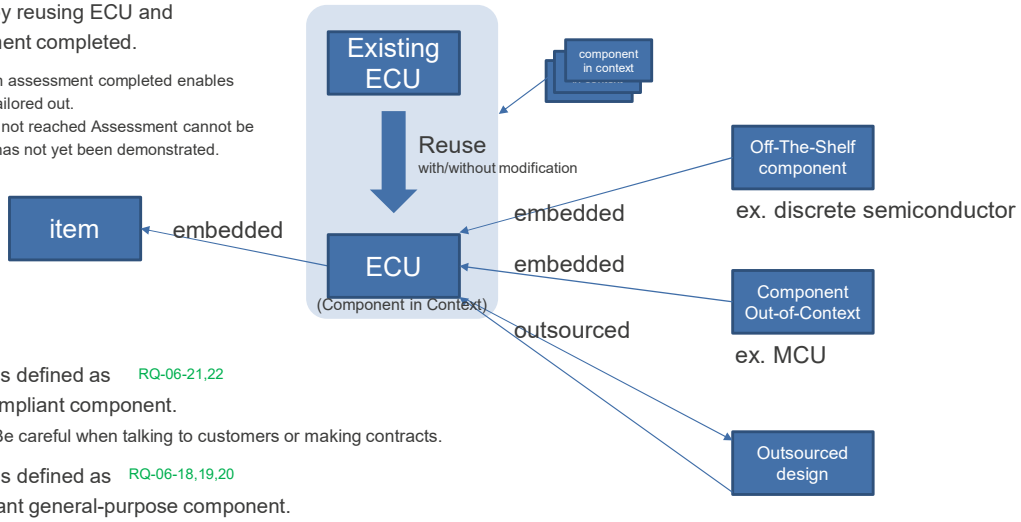
WP ID	Name
WP-06-01	Cybersecurity plan

COMPONENT*1 AND REUSE

*1: "Component" is not equal to "Component" defined in ISO 26262, is equal to "element" in ISO 26262.

RQ-06-15,16,17

- Dev-cost can be reduced by reusing ECU and component which assessment completed.
  - ✓ Reusing WPs of the ECU which assessment completed enables corresponding activities to be tailored out.
  - ✓ ECU and component that have not reached Assessment cannot be Reused as 21434 compliance has not yet been demonstrated.



- Off-The-Shelf Component is defined as an ISO/SAE 21434 non-compliant component. RQ-06-21,22
  - It is not a so-called COTS. Be careful when talking to customers or making contracts.
- Component out of context is defined as an ISO/SAE 21434 compliant general-purpose component. RQ-06-18,19,20
- Cybersecurity plan should be tailored based on the examination of reqs for components used and the application of "Reuse".

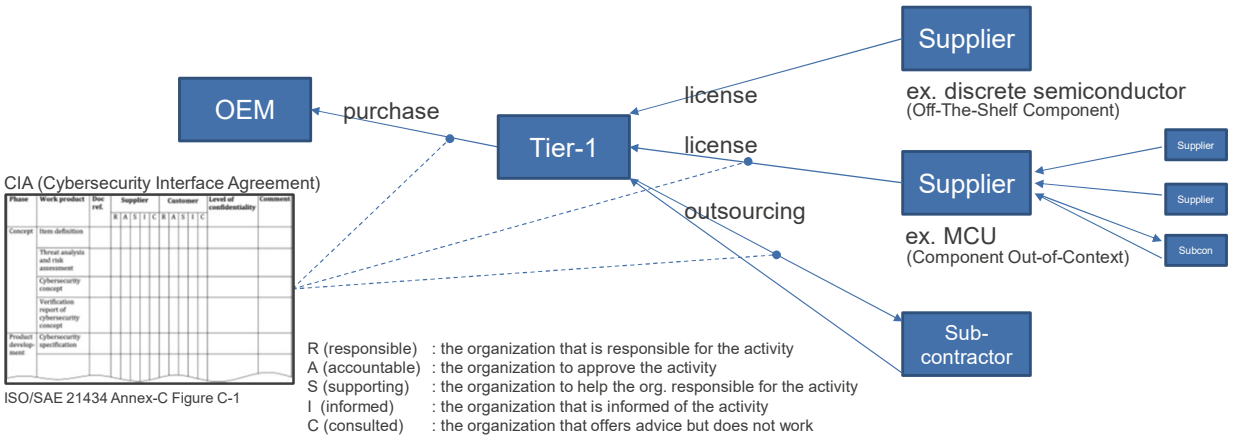
An item equivalent to a system incorporates components in context, such as ECUs, that are developed based on the context of that system.
In addition to components in context, an ECU incorporates off-the-shelf components such as discrete semiconductors, components out of context such as microcontrollers, and outsourced parts.
In ISO/SAE 21434, off-the-shelf component is defined as a component that does not comply with ISO/SAE 21434.
Please note that they are not necessarily COTS.
On the other hand, component out of context is defined as a general purpose component that complies with ISO/SAE 21434.
ECUs and components that have completed assessment can be reused to reduce development efforts.
The incorporation and reuse of each component has its own requirements that must be complied with, and these must be examined in order to tailor a security plan.

WP ID	Name
WP-07-01	Cybersecurity Interface Agreement (CIA)

DISTRIBUTED DEVELOPMENT

If cybersecurity activities are distributed to other parties, **their cybersecurity capability** shall be checked. RQ-07-01

If both parties develop according to ISO/SAE 21434 compliant process, the **division of responsibilities** shall be defined **as CIA**. RQ-07-04



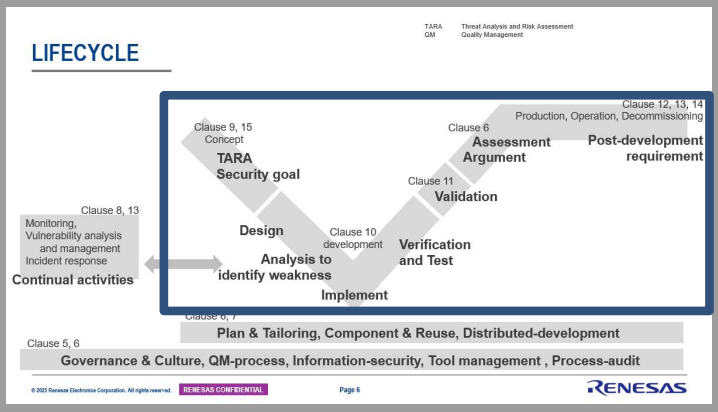
CIA (Cybersecurity Interface Agreement)

ISO/SAE 21434 Annex-C Figure C-1

R (responsible) : the organization that is responsible for the activity
A (accountable) : the organization to approve the activity
S (supporting) : the organization to help the org. responsible for the activity
I (informed) : the organization that is informed of the activity
C (consulted) : the organization that offers advice but does not work

In product development, components may be introduced from outside companies.
In some cases, parts may be outsourced to a subcontractor.
The developed product is then delivered to the customer.
In such cases, first check the company's cybersecurity capabilities.
Check whether the company has the capabilities for the process foundations described at the end of this tutorial and whether the company has a development process that complies with ISO/SAE 21434.
If the company has a development process that complies with ISO/SAE 21434, clarify the responsibilities between the company and your company for each work product defined in ISO/SAE 21434.
To clarify responsibilities, a document called a Cybersecurity Interface Agreement is generally used.
R,A,S,I,C RASIC of each company for each work product are determined.
Note that "A" stands for accountable, but it means the company that approves the work product.

DEVELOPMENT



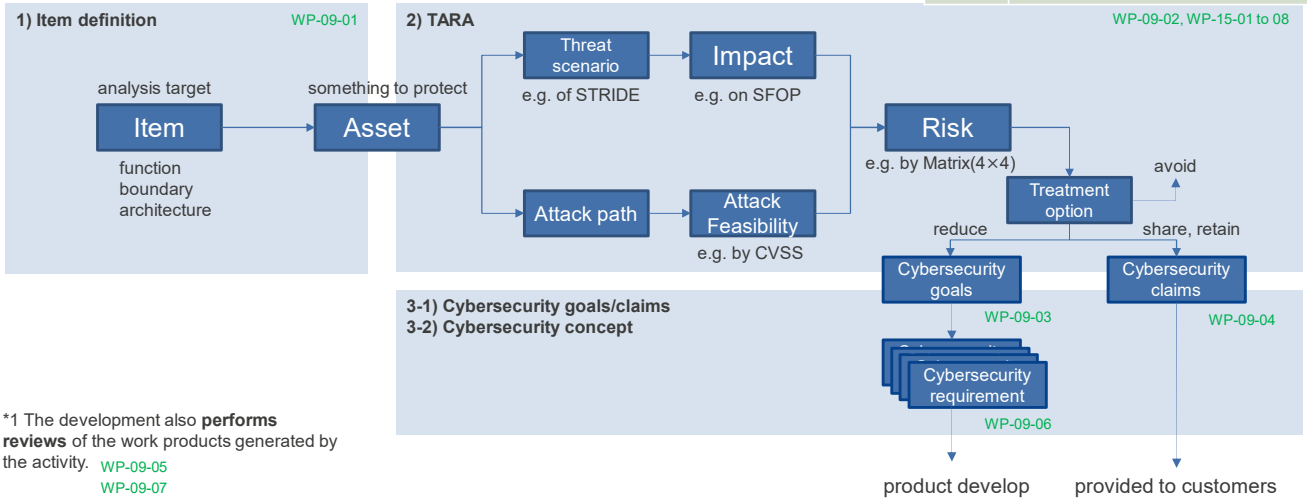
This chapter explains the requirements for each security activity in accordance with the V model of product development.

CONCEPT PHASE
TARA AND CYBERSECURITY CONCEPT

TARA	Threat Analysis and Risk Assessment
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
SFOP	Safety, Financial, Operational, Privacy
CVSS	Common Vulnerability Scoring System

WP ID	Name
WP-09-01	Item definition
WP-09-02	TARA (Detail: Clause 15)
WP-09-03	Cybersecurity goals
WP-09-04	Cybersecurity claims
WP-09-05	Verification report for cybersecurity goals
WP-09-06	Cybersecurity concept
WP-09-07	Verification report for the cybersecurity concept

TARA is performed then **Cybersecurity Requirements** are identified *1.



*1 The development also **performs reviews** of the work products generated by the activity. WP-09-05 WP-09-07

In the concept phase, an item is defined, and threats to assets and their impact, as well as attack paths and feasibility are analysed.
If risks identified as a result of the analysis are to be reduced, the corresponding cybersecurity goals are clarified.
If they are to be shared or retained, they are clarified as cybersecurity claims.
Each cybersecurity goal is broken down into cybersecurity requirements for the product.

DEVELOPMENT PHASE (1)
DESIGN AND WEAKNESS-IDENTIFICATION

CERT Computer Emergency Response Team
MISRA Motor Industry Software Reliability Association

WP ID	Name
WP-10-01	Cybersecurity specifications
WP-10-03	Documentation of the modelling, design, or programming languages and coding guidelines
WP-10-04	Verification report for the cybersecurity specifications
WP-10-05	Weaknesses found during product development

Design Specifications are created by applying design principles *1 . WP-10-01

Weaknesses which may lead to a vulnerability are identified.

WP-10-03, RQ-10-04, 05, 07

examples of design principles :

- Modularity, abstraction and encapsulation
- Use of structured constructs
- Trusted design & implementation (cf. NIST Special Publication 800-160 F.1)
- Resilience of language against vulnerabilities
- Secure coding (e.g. CERT-C, MISRA-C)

WP-10-05, RQ-10-07, RC-10-12

identifying weaknesses :

- Weaknesses can be identified using the results of vulnerability analysis and management*2, a part of "continuous security activities" carried out in parallel with product development.
- Weaknesses can also be identified using the results of tests*3, such as penetration tests conducted during the verification phase.

*1 Verification is also performed for the design specification. WP-10-04
Verification includes review, analysis, simulation and prototyping in ISO/SAE 21434. RQ-10-08
*2 Vulnerability analysis and management are defined at clause 8: “continuous cybersecurity activities”, not at clause 10: “product development” in ISO/SAE 21434.
*3 Testing is also explained at the next slide “Development (Verification and Validation).

In the development phase, design principles are applied and design specifications are created.
Verification requirements for the design specifications are also defined, and verification here refers to reviews.
ISO/SAE 21434 considers not only simulations but also reviews to be a form of verification.
For secure coding, one of the design principles examples such as CERT-C and MISRA-C are given.
In addition, during the design phase, weaknesses that could lead to vulnerabilities are identified.
Weaknesses can be identified using the results of vulnerability analysis and management carried out as part of continual activities or
the results of penetration testing carried out in the verification phase.

DEVELOPMENT PHASE (2)
VERIFICATION AND VALIDATION

WP ID	Name
WP-10-06	Integration and verification specification
WP-10-07	Integration and verification report
WP-11-01	Validation report

Verification to ensure that cybersecurity specifications have been implemented is performed during development.

Validation to confirm the validity and achievement of security goals and claims is performed at the vehicle level*1.

WP-10-06, 07, RQ-10-10, RC-10-12

example of verification :
- requirements-based test
- interface test / resource usage evaluation
- control flow & data flow / dynamic analysis & static analysis

example of methods for deriving test cases :
- analysis of requirements
- analysis of equivalence classes, boundary value
- guessing based on knowledge or experience

example of testing to confirm unidentified weaknesses and vulnerabilities remaining are minimized :
- penetration testing
- fuzz testing
- functional testing

WP-11-01

validation activities shall confirm :
- adequacy of cybersecurity goals
- achievement of cybersecurity goals
- validity of cybersecurity claims
- validity of the requirements on the operational environment

verification activities are done by :
- reviewing WPs of sub-clause 9.5 and clause 10.
- penetration testing to demonstrate appropriateness and achievement of cybersecurity goals.
- reviewing all managed risks identified through clause 9, 10.

*1: In ISO/SAE 21434, validation is defined in a narrower sense than the general term.

Verification is an activity that ensures that a product is implemented according to specifications.
Testing and penetration testing to ensure that weaknesses are minimised are also listed as kinds of verification in ISO/SAE 21434.
Validation, on the other hand, is an activity that ensures that cybersecurity goals are adequate and achieved and that cybersecurity claims are valid.
Validation is performed at the vehicle level.
Note that ISO/SAE 21434 defines validation in a narrower sense than the general term.

POST-DEVELOPMENT REQUIREMENT
PRODUCTION / OPERATION / DECOMMISSION

WP ID	Name
WP-06-04	Release for post-development report
WP-10-02	Cybersecurity requirements for post-development
WP-12-01	Production control plan
WP-14-01	Procedures to communicate the end of cybersecurity support

Post-development requirements include the requirements for production, operation and decommissioning.

WP-12-01

Production :

- The following requirements for secure production shall be included in the production control plan:
  - Tool and equipment management
  - Security asset management
- Development team shall confirm in advance that the above management will be implemented reliably in production sites.

WP-10-02, RQ-13-03, WP-14-01

Operation :

- During operations, manuals, their updates, and support to properly implement and initialize the system shall be provided.
- Procedures to communicate the end of cybersecurity support shall be in place.
- Incident response carried out during operations will be explained in the chapter "Continuous activities".

RQ-14-02

Decommissioning :

- Proper guidance and instructions for decommissioning shall be provided.

Before moving from the development phase to the production/operation phase, the development team shall clarify above post-development requirements. WP-06-04

ISO/SAE 21434 defines the requirements for production, operation and decommission together as post-development requirements.
For production, it requires that the production control plan created in the QM process includes the management of tools and equipment
as well as the management of security assets.
The development team must confirm that these controls are being implemented reliably before production starts.
For operation, manuals, updates, and support must be provided to ensure correct system implementation and initialization.
Regarding support, a procedure to communicate the end of cybersecurity support must be defined.
For decommission, it is also required to provide appropriate instructions and guides.

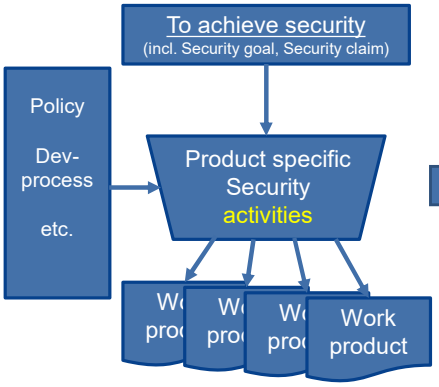
WP ID	Name
WP-06-02	Cybersecurity case

CYBERSECURITY CASE

Create a **cybersecurity case** as an argument to show that product security has been achieved.[WP-06-02]

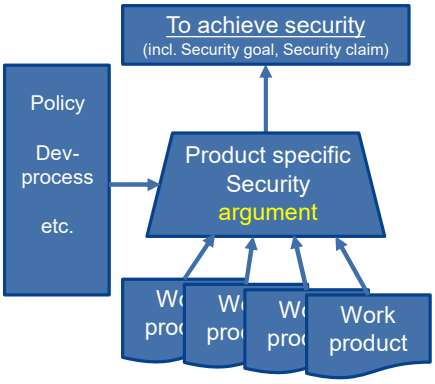
Product development

Create WPs based on sec goals, claims & dev-process.



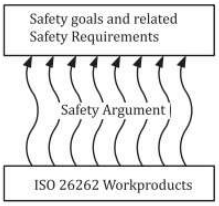
Security case creation

Create the argument to achieve sec goals & claims.



cf. Safety case (ISO 26262 part-10)

Direction of the arrow is important.



6.4.8.1 A safety case shall be developed, in accordance with the safety plan, in order to provide the argument for the achievement of functional safety.

6.4.8.2 The safety case should progressively compile the work products that are generated during the safety lifecycle to support the safety argument.

✓ Most OEMs and Tier1s use **GSN** (Goal Structure Notation, ex. A Systematic Approach to Safety Case Management) or its extended version.

Once product development is completed, a cybersecurity case is created.
Product development is the activity of creating work products in line with the development process toward the goal of achieving cybersecurity for the product, while a cybersecurity case is the activity of creating an argument that shows that the work products have achieved cybersecurity for the product.
OEM and Tier-1 often create arguments using GSN, Goal Structure Notation.

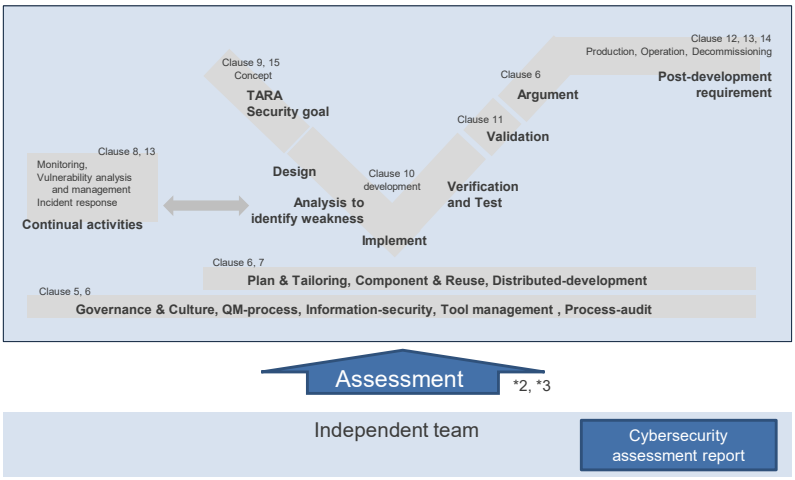
WP ID	Name
WP-06-03	Cybersecurity assessment report

CYBERSECURITY ASSESSMENT

WP-06-03

Independent team*1 checks the plan, planned WPs, and Security case to confirm that product's security has been achieved.

✓ While Security case is a confirmation by development team that the product's security has been achieved, Assessment is a confirmation by an independent team.



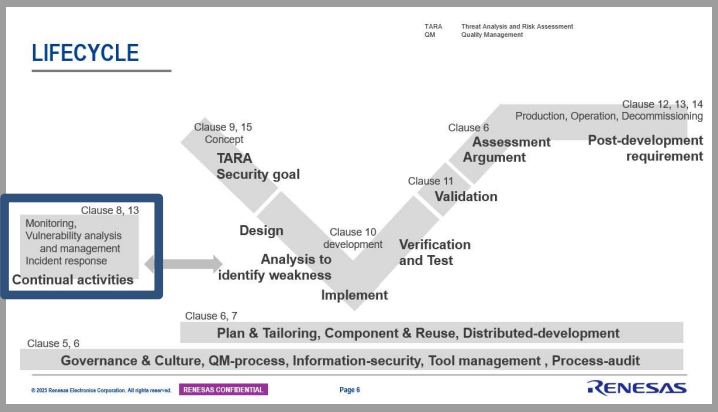
*1 In ISO/SAE 21434, team independency is defined in case of assessment only - not review, verification, testing, validation, audit, etc.

*2 Cybersecurity assessment can be performed in incremental steps. RQ-06-26

*3 Cybersecurity assessment is neither a Certification nor an Audit.

Once the cybersecurity case is created, an independent team performs a cybersecurity assessment, if necessary.
Whereas a cybersecurity case is a confirmation by the development team of cybersecurity achievements, an assessment is a confirmation by an independent team.
The assessment reviews the plan, the planned work products and the cybersecurity case.
In ISO/SAE 21434, team independence is defined only for cybersecurity assessments, not for reviews, verifications, testing, validations, audits, etc.
Also, cybersecurity assessments are different from certifications and audits.

CONTINUAL SECURITY ACTIVITIES



This chapter describes the continual cybersecurity activities that are conducted in parallel with the development of each product.

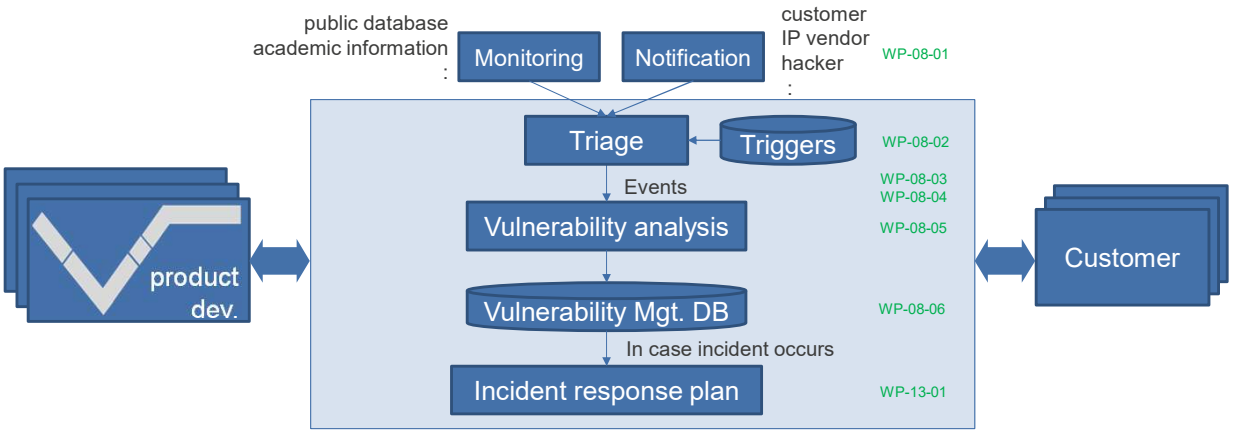
CONTINUAL SECURITY ACTIVITIES

WP ID	Name
WP-08-01	Selected sources for cybersecurity monitoring
WP-08-02	Triggers
WP-08-03	Cybersecurity events
WP-08-04	Weakness from cybersecurity events
WP-08-05	Vulnerability analysis
WP-08-06	Evidence of managed vulnerabilities
WP-13-01	Cybersecurity incident response plan

The organization monitors or is notified of cybersecurity information sources.

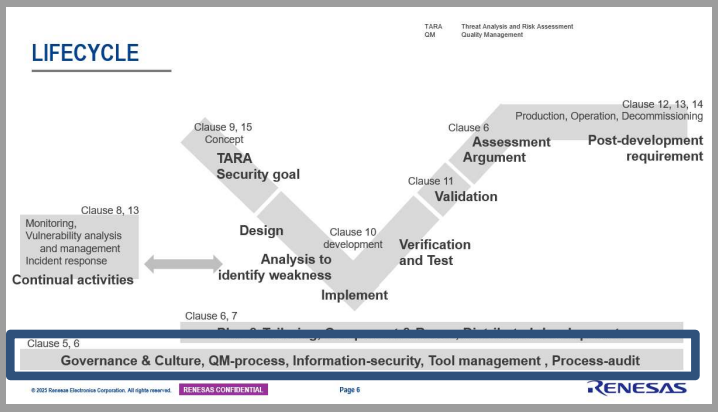
Triages information and analyzes and manages vulnerabilities.

When an incident occurs, develops a response plan.



The organization monitors public databases, receives notifications from customers and hackers, triages the information, and analyses and manages vulnerabilities.
If a managed vulnerability becomes an incident, a response plan must be created for each incident.

FOUNDATION OF SECURITY PROCESS



This chapter describes the requirements that are the foundation of the cybersecurity process.

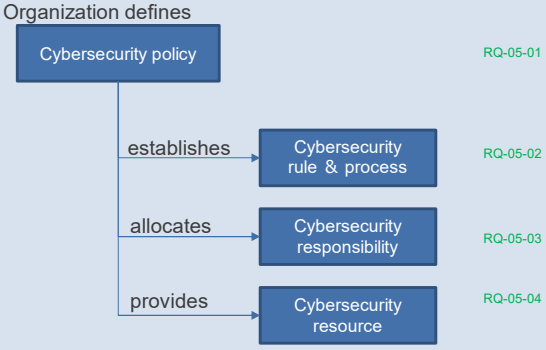
GOVERNANCE AND CULTURE

WP ID	Name
WP-05-01	Cybersecurity policy, rules and processes
WP-05-02	Evidence of competence management, awareness management and continuous improvement

Cybersecurity Governance

WP-05-01

Organization defines



RQ-05-05

✓ Organization shall establish and maintain communication channels with cybersecurity-related disciplines, such as FuSa.

Cybersecurity Culture WP-05-02

Organization shall foster & maintain strong cybersecurity culture. RQ-05-06, 07, 08

Examples (excerpt from Annex-B)

- Cybersecurity personnel act as role models with a good sense for appropriateness and practical implementation that leads to trust in their actions by the entire organization.
- Cybersecurity issues are discovered and resolved from the earliest stage in the product lifecycle.
- The organization is prepared to react fast to vulnerabilities or incidents in the field.
- The required resources for cybersecurity are allocated. Skilled resources have the competence commensurate with the activity assigned.
- The process uses diversity to its advantage.
- The discovery and resolution process continues in the field, in manufacturing and in development of other products.
- Continuous improvement is integral to all processes.
- Defined, traceable, and controlled processes are followed.

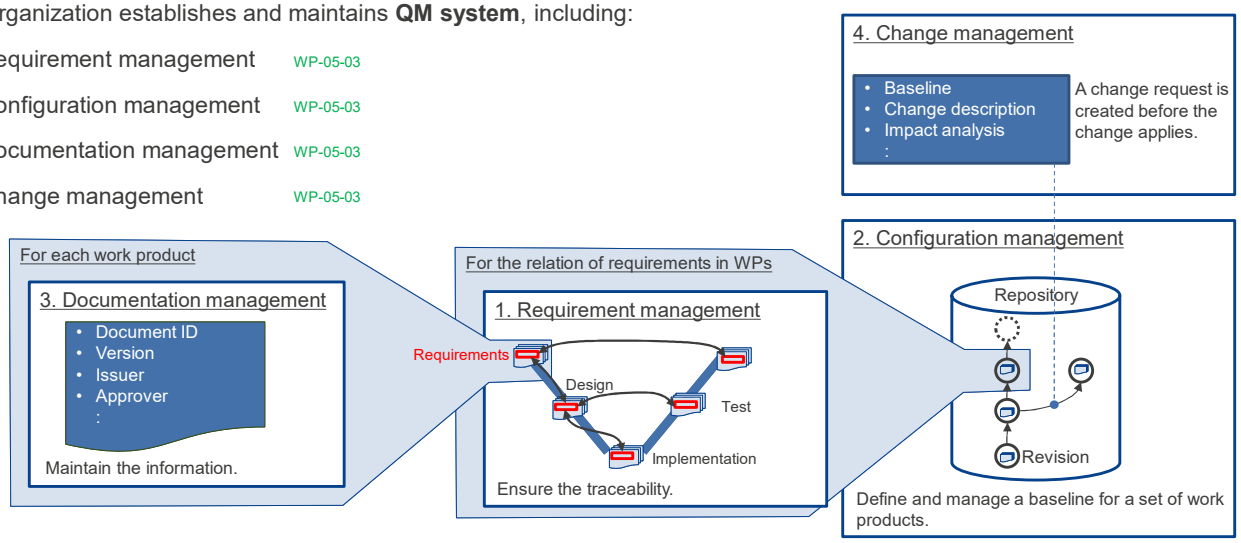
To establish cybersecurity governance, the organization defines cybersecurity policy, creates rules and processes, allocates responsibilities and provides resources.
Organization must also foster and maintain a strong cybersecurity culture.
In addition to ensuring the skills of personnel and organizational competencies, continuous improvement of rules and fast reaction to incidents, organization must also continually work to discover and resolve problems.

WP ID	Name
WP-05-03	Evidence of the organization's management systems

QM PROCESS

The organization establishes and maintains **QM system**, including:

1. Requirement management WP-05-03
2. Configuration management WP-05-03
3. Documentation management WP-05-03
4. Change management WP-05-03



The organization establishes and maintains a quality management system. Requirements management, configuration management, document management and change management also must be properly implemented.

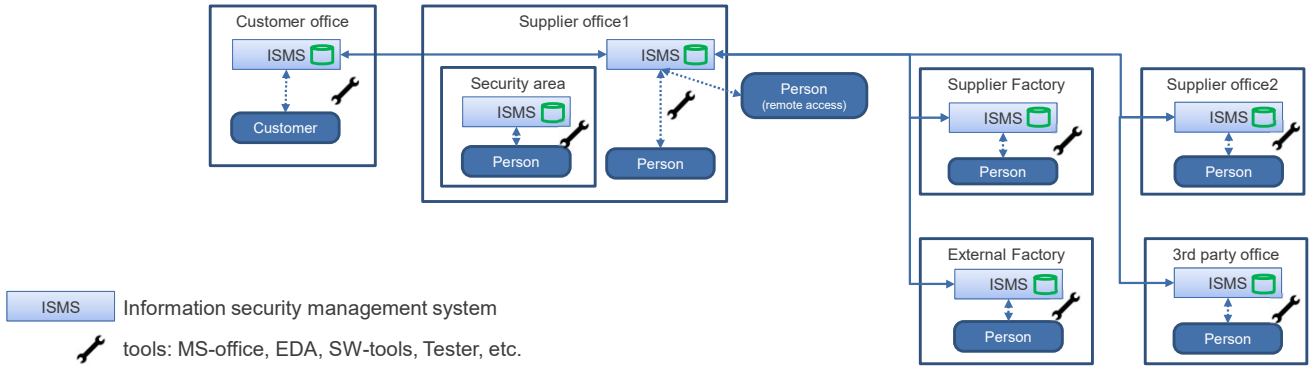
ISMS Information Security Management System

WP ID	Name
WP-05-03	Evidence of the organization's management systems
WP-05-04	Evidence of tool management

INFORMATION SECURITY AND TOOL

Organization manages **information security.** WP-05-03

Organization manages **tools** that can influence the cybersecurity of products. WP-05-04



ISMS Information security management system

tools: MS-office, EDA, SW-tools, Tester, etc.

electrical or physical assets: design-data, drawings, instructions, wafers, ECUs, etc.

Person Persons

Information-access, Sending and receiving mail, parcels, etc.

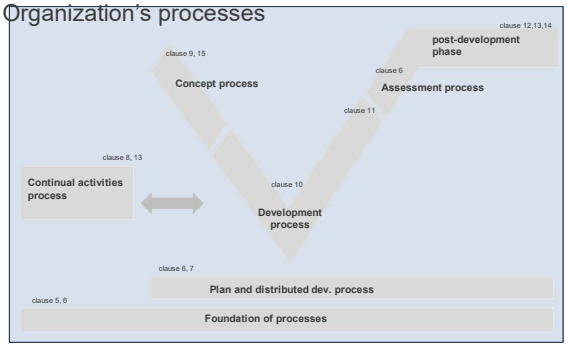
In addition to QM processes, information security is also important as a foundation for cyber security management in product development.
It is also necessary to manage tools and equipment that can influence the cybersecurity of the product, such as documentation tools, EDA, compilers and testers.
The organization needs to ensure that information security and tools are properly managed not only in the direct visible area but also in factories, subcontractors, suppliers, etc. to prevent leakage or tampering of their electronic and physical assets.

WP ID	Name
WP-05-05	Organizational cybersecurity audit report

CYBERSECURITY AUDIT

Organization audits whether its processes comply with ISO/SAE 21434 *1,*2,*3. WP-05-05

Organization's processes



Audit compliance

ISO/SAE 21434 requirements and WPs

Clause	Req.	WP
5. Organizational cybersecurity management	17	5
6. Project dependent cybersecurity management	34	4
7. Distributed cybersecurity activities	8	1
8. Continual cybersecurity activities	8	6
9. Concept	11	7
10. Product development	13	7
11. Cybersecurity validation	2	1
12. Production	3	1
13. Operations and maintenance	3	1
14. End of cybersecurity support and Decommissioning	2	1
15. Threat analysis and risk assessment methods	17	8
	118	42

Organizational cybersecurity audit report

*1 ISO/SAE 21434 does not define the independence of the audit team.

*2 ISO/SAE 21434 does not require external certification, but this requirement can be substituted with external certification.

*3 This requirement is not the same type of audit as the functional safety audit defined in ISO 26262.

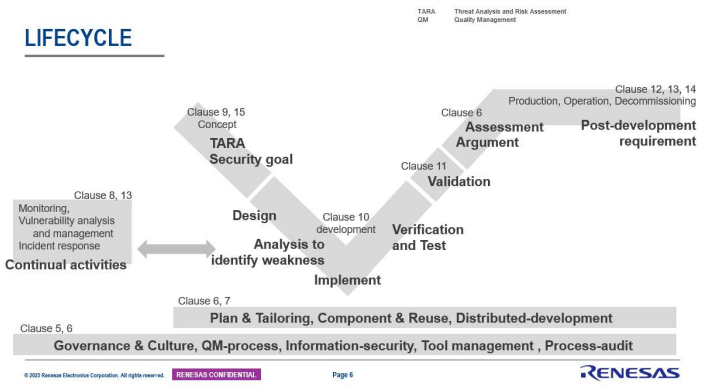
The organization audits their processes, which they have tailored to suit their organization to ensure that they comply with the requirements of ISO/SAE 21434 and compiles the results in an organizational cybersecurity audit report as evidence of compliance.
ISO/SAE 21434 does not require external certification by a third party, but external certification can be used as an alternative for the organizational cybersecurity audit report.

SUMMARY

This is a summary.

SUMMARY

The ISO/SAE 21434 - Road vehicles Cybersecurity engineering - consists of the following clauses.
The clauses define requirements and work products.



Clause	Req.	WP
5. Organizational cybersecurity management	17	5
6. Project dependent cybersecurity management	34	4
7. Distributed cybersecurity activities	8	1
8. Continual cybersecurity activities	8	6
9. Concept	11	7
10. Product development	13	7
11. Cybersecurity validation	2	1
12. Production	3	1
13. Operations and maintenance	3	1
14. End of cybersecurity support and Decommissioning	2	1
15. Threat analysis and risk assessment methods	17	8
	118	42

In ISO/SAE 21434, the requirements explained in this tutorial are defined in clauses 5 to 15. Clause 1 describes the scope, clause 2 describes the normative references, clause 3 explains terms and abbreviations, and clause 4 provides an overview of cybersecurity risk management as a general consideration.

APPENDIX

In Appendix,

TERMS (EXCERPT FROM ISO/SAE 21434 CLAUSE 3)

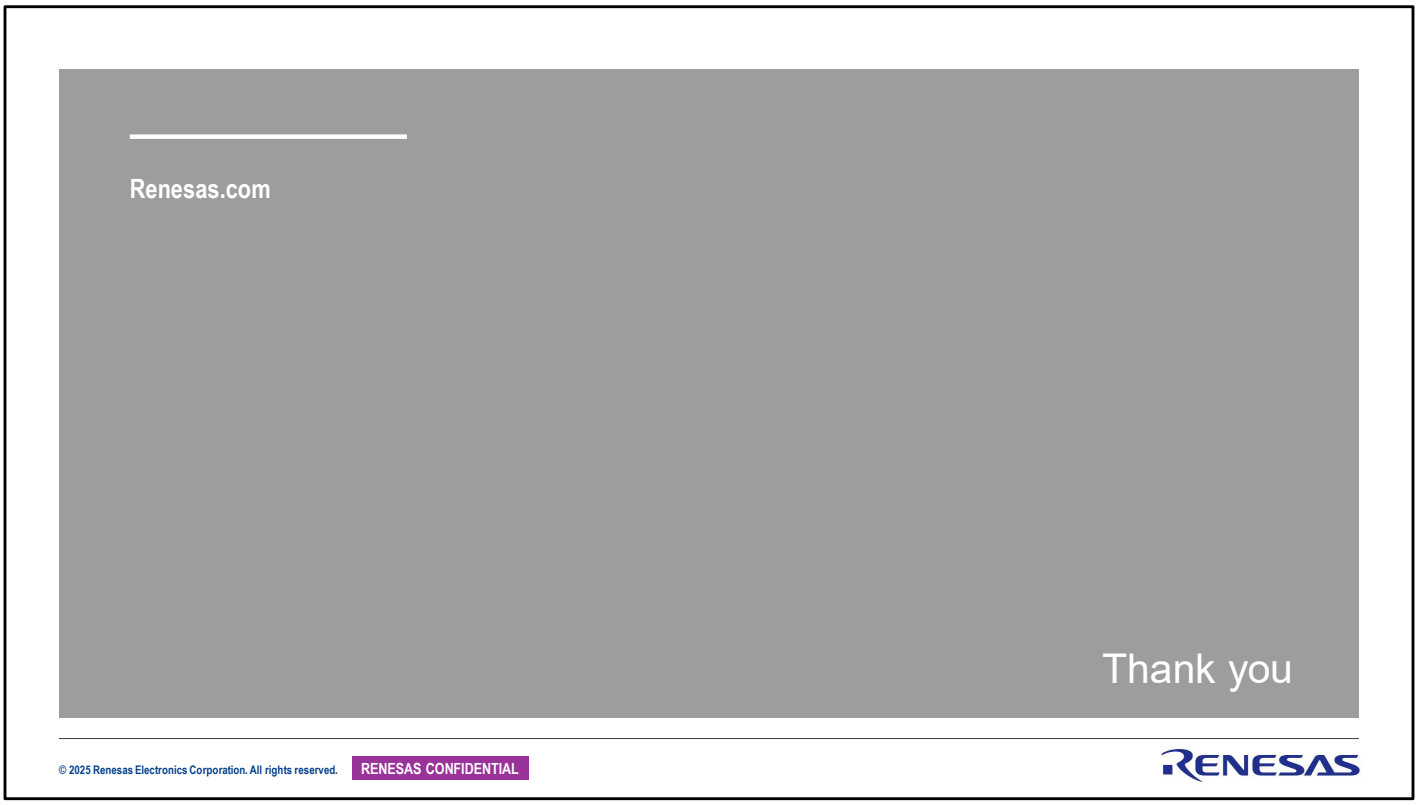
Term	Description	Term	Description
Asset	object that has value, or contributes to value	Damage scenario	adverse consequence involving a vehicle or vehicle function and affecting a road user
Attack feasibility	attribute of an attack path describing the ease of successfully carrying out the corresponding set of actions	Impact	estimate of magnitude of damage or physical harm from a damage scenario
Audit	examination of a process to determine the extent to which the process objectives are achieved	Item	component or set of components that implements a function at a vehicle level
Component	part that is logically and technically separable	Out of context	not developed in the context of a specific item
Cybersecurity	condition in which assets are sufficiently protected against threat scenarios to items of road vehicles, their functions and their electrical or electronic components	Risk	effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact
Cybersecurity assessment	judgement of cybersecurity	Tailor	to omit or perform an activity in a different manner compared to its description in this document
Cybersecurity case	structured argument supported by evidence to state that risks are not unreasonable	Threat scenario	potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario
Cybersecurity claim	statement about a risk, including a justification for retaining or sharing the risk.	Triage	analysis to determine the relevance of cybersecurity information to an item or component
Cybersecurity concept	cybersecurity requirements for the item and requirements on the operational environment with associated information on cybersecurity controls	Validation	confirmation, through the provision of objective evidence, that the cybersecurity goal of the item are adequate and are achieved
Cybersecurity incident	situation in the field that can involve vulnerability exploitation	Verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
Cybersecurity goal	concept level cybersecurity requirement associated with one or more threat scenarios	Vulnerability	weakness that can be exploited as part of an attack path
Cybersecurity specification	cybersecurity requirements and corresponding architectural design	Vulnerability analysis	systematic identification and evaluation of vulnerabilities

definitions of terms and

ABBREVIATIONS (USED IN THIS TUTORIAL)

Abbreviation	Description
CERT	Computer Emergency Response Team
CIA	Cybersecurity Interface Agreement
CVSS	Common Vulnerability Scoring System
E/E	Electrical and Electronic
ECU	Electronic Control Unit
FuSa	Functional Safety
HW	Hardware
ISMS	Information Security Management System
MISRA	Motor Industry Software Reliability Association
OEM	Original Equipment Manager
QM	Quality Management
RASIC	Responsible, Accountable, Supporting, Informed, Consulted
RC	Recommendation
RQ	Requirement
SFOP	Safety, Financial, Operational, Privacy
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
SW	Software
TARA	Threat Analysis and Risk Assessment
WP	Work Product

the abbreviations are explained, but



it would be a good idea to go back and read any parts skipped over in the explanation.
Thank you very much for participating in this tutorial for the introduction of ISO/SAE 21434.